INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 00.004 https://doi.org/10.23947/1992-5980-2018-18-3-333-338

Selecting safety package components of enterprise information system following requirements of standard legal documents*

E. A. Vitenburg [1], A. A. Levtsova [2]**

[1, 2] Volgograd State University, Volgograd, Russian Federation

Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов***

Е. А. Витенбург[1], А. А. Левцова[2]**

[1, 2] Волгоградский государственный университет, г. Волгоград, Российская Федерация

Introduction. Production processes quality depends largely on the management infrastructure, in particular, on the information system (IS) effectiveness. Company management pays increasingly greater attention to the safety protection of this sphere. Financial, material and other resources are regularly channeled to its support. In the presented paper, some issues on the development of a safety enterprise information system are considered.

Materials and Methods. Protection of the enterprise IS considers some specific aspects of the object, and immediate threats to IT security. Within the framework of this study, it is accepted that IS are a complex of data resources. A special analysis is resulted in determining categories of threats to the enterprise information security: hacking; leakage; distortion; loss; blocking; abuse. The connection of these threats, IS components and elements of the protection system is identified. The requirements of normative legal acts of the Russian Federation and international standards regulating this sphere are considered. It is shown how the analysis results enable to validate the selection of the elements of the IS protection system.

Research Results. A comparative analysis of the regulatory literature pertinent to this issue highlights the following. Different documents offer a different set of elements (subsystems) of the enterprise IS protection system. To develop an IS protection program, you should be guided by the FSTEC Order No. 239 and 800-82 Revision 2 Guide to ICS Security.

Discussion and Conclusions. The presented research results are the basis for the formation of the software package of intellectual support for decision-making under designing an enterprise information security system. In particular, it is possible to develop flexible systems that allow expanding the composition of the components (subsystems).

Введение. Качество производственных процессов во многом зависит от инфраструктуры управления — в частности, от эффективности информационной системы (ИС). Менеджмент компаний уделяет все большее внимание обеспечению безопасности этой сферы, на ее поддержку регулярно направляются финансовые, материальные и другие ресурсы. В представленной работе рассмотрены вопросы построения комплекса защиты информационной системы предприятия.

Материалы и методы. Охрана ИС предприятия учитывает особенности объекта защиты и актуальные угрозы информационной безопасности. В рамках данного исследования принято, что ИС представляет собой комплекс информационных ресурсов. По результатам специального анализа определены категории угроз информационной безопасности предприятия: взлом; утечка; искажение; утрата; блокирование; злоупотребление. Выявлена связь данных угроз, компонентов ИС и элементов комплекса защиты. Рассмотрены требования нормативно-правовых актов Российской Федерации и международных стандартов, регулирующих данную сферу. Показано, каким образом результаты данного анализа позволяют обосновать выбор элементов комплекса защиты ИС.

Результаты исследования. Сравнительный анализ регламентирующей литературы, относящейся к данному вопросу, позволил выявить следующее. Разные документы предлагают разный набор элементов (подсистем) комплекса защиты ИС предприятия. Разрабатывая программу защиты ИС, следует руководствоваться Приказом ФСТЭК № 239 и стандартом 800-82 Revision 2 Guide to ICS Security.

Обсуждение и заключения. Результаты представленного исследования являются основой для формирования программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии. В частности, можно разрабатывать гибкие комплексы, позволяющие расширять состав элементов (подсистем).

* The research is done with the financial support from the Russian Federation President Council on Grants within the frame of R&D “Building a model of intellectual support for decision-making when designing an enterprise information security system”.

** E-mail: e.vitenburg@ec-rs.ru, alexandra.levtsova@yandex.ru

*** Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации в рамках НИР «Построение модели интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии».

Keywords: information system, information security, information security system, information security subsystems.

Ключевые слова: информационная система, информационная безопасность, система защиты информации, подсистемы защиты информации.

For citation: E.A. Vitenburg , A.A. Levtsova. Selecting safety package components of enterprise information system following requirements of standard legal documents. Vestnik of DSTU, 2018, vol. 18, no.3, pp. 333−338. https://doi.org/10.23947/1992-5980-2018-18-3-333-338

Образец для цитирования: Витенбург, Е. А. Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов / Е. А. Витенбург, А. А. Левцова // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 3. — С. 333−338. https://doi.org/10.23947/1992-5980-2018-18-3-333-338

Introduction. Information systems (IS) are increasingly used in the production and management processes. Accordingly, the problem of cyber security (CS) of IS gets worse. In particular, IS weak isolation simplifies an unauthorized access to them [1, 2, 3]. The consequences of fraudulent attacks on IS may be production downtime, financial losses, and on the worst-case scenario – even man-made disasters [4]. Thus, the crucial task is to establish a protective system for the industrial IS which could effectively militate against malicious acts.

Materials and Methods. The development of an information security system is based on the results of a pre-project study during which the setup of the asset to be protected and the immediate threats are determined.

The asset of protection is represented as a set of information resources:

$$Object_{\text{Sec}} = \{NE, CC, IS, Sts, WS, PE, OS, SS, AS, IP, Sn, RSM, SM, IA\}.$$

Here, NE is a set of network hardware; CC is a number of communications lines; IS is an array of infrastructure servers; Sts a set of data storage systems; WS is number of localhosts; PE is a number of external equipment; OS is an array of operating systems; SS is a set of system software; AS is a set of application software; IP is number of information processes running in the tech companies; Sn is subnets; RSM is a number of removable media; SM is electronic data storage devices; IA is information assets.

Number of immediate CS threats $Threat$ is determined [5]:

$$Threat = \{Breaking, Leak, Distortion, Loss, Blocking, Abuse\}.$$

Here, $Breaking$ is hacking threats; $Leak$ is information leakage threatening; $Distortion$ is threats of distortion; $Loss$ is threats of loss; $Blocking$ is threats of blocking the information resources of a tech company; $Abuse$ is risks of abuse.

The system which meets these threats is an enterprise IP protection system (ISPS) (Fig. 1).

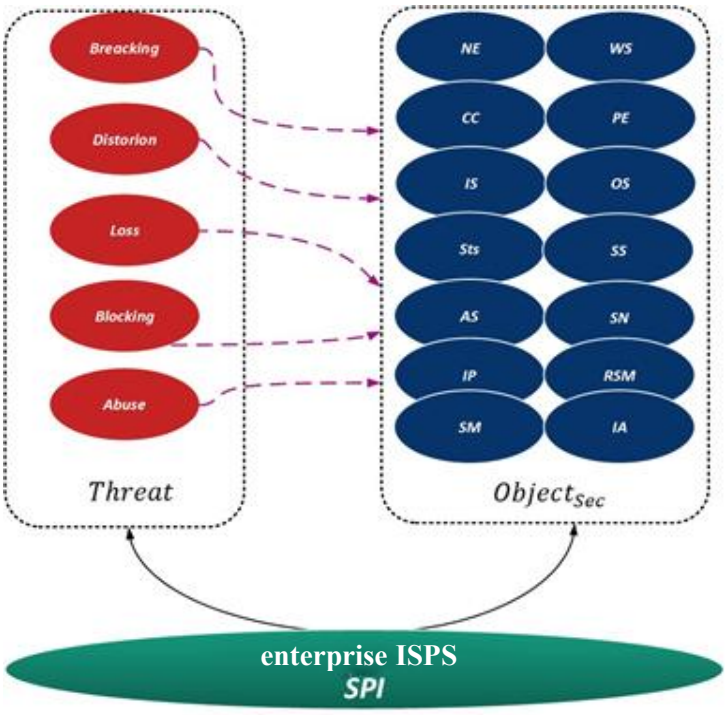

Fig. 1. Security objects – threats relations in ISPS diagram

SPI (*system of protection of information*) is two-tiered, and it includes subsystems (components) [6]:

— a set of subsystems (*Subsystem*) of information security;

— number of information security facilities (*MP*, *means of protection*).

Fig. 2 shows a general form of the ISPS structure.

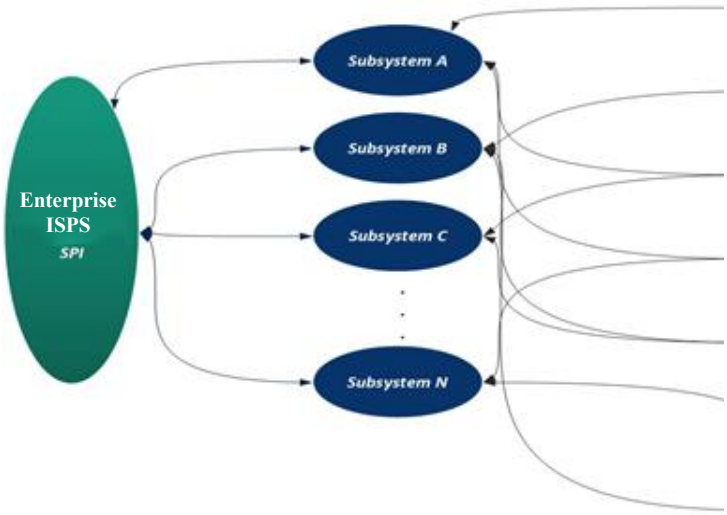

Fig. 2. Generalized structure of enterprise ISPS

When determining the components of the information protection system, experts proceed from the analysis of available regulatory documentation and standards operating at the enterprise. International experience should be taken into account as well. 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security [1] is widely used in the foreign and domestic practice. This standard was developed by the US National Institute of Standards and Technology. It, in particular, contains recommendations on improving safety in the industrial inspection systems, including the supervisory control and data acquisition systems. It shows how the organizational processes and business functions are subjected to threats, and it describes usual vulnerabilities. Special attention is given to security measures and counters that should be undertaken in a hostile situation.

Research Results. Domestic regulatory legal acts (RLA) handling the enterprise IS protection can be conditionally divided into two categories [6]:

— RLA on maintenance of information safety of the automatic process control system (APCS);

- RLA on the security of critical information infrastructure (CII).

Crucially, vulnerabilities in the CII protection can cause major material and environmental damage. Inadequate CII protection is fraught with social and military-political problems.

Designing the information security system (in particular, when modeling the intellectual support for decision-making) requires a preliminary comparative analysis of the profile regulatory legal acts of the Russian Federation. As for example, the following documents should be considered:

— Order no. 31 of the Federal Service for Technology and Export Control (FSTEC of Russia) of March 14, 2014, "On Approving Requirements for Providing Information Protection in Automated Control Systems of Production and Technological Processes at Critical Objects, Potentially Hazardous Facilities, and Objects posing high threat to life and health of people and the environment" [7];

— Order no. 239 of FSTEC of Russia of December 25, 2017, "On Approval of Requirements for Ensuring the Security of Significant Facilities of the Information Infrastructure of the Russian Federation" (draft) [8];

— International standard 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security [9].

Comparative analysis of the Orders of FSTEC of Russia no. 31 and no. 239 is presented in Table 1.

Table 1

Elements (subsystems) of enterprise IS protection system in Orders of FSTEC no. 31 and no. 239

	FSTEC Order no. 31 of 14.03.14	FSTEC Order no. 239 of 25.12 2017
ISPS Subsystems	Identification and authentication of access subjects and access objects (IAF)	
	Access control of access subjects and access objects (UPD)	
	Restriction of software environment (OPS)	
	Protection of machine-readable media (ZNI)	
	Secure event logging (RSB)	Security audit (AUD)
	Antivirus protection (AVZ)	
	Intrusion detection (OV)	Intrusion prevention (PV)
	Infosecurity control (analysis) (ANZ)	Protection of information (automated) system and its components (ZIS)
	Integrity control (OTsL)	
	Information assurance (ODT)	
	Event planning to ensure information protection (PLN)	
	Protection of technical facilities and systems (ZTS)	
	Security assurance of software development (OBR)	Information security incident response (INTs)
	Virtualization environment protection (ZSV)	Personnel informing and training (IPO)
	Software update control (OPO)	
	Security protection of emergency procedures (DNS)	
	Analysis of threats to information security and risks from their implementation (UBI)	—
	Configuration control of data processing system and its security system (UKF)	
Note. For greater clarity, variances are not only placed in different cells, but are also highlighted in gray		

So, FSTEC Order no. 239 provides for the following subsystems in the IS protection system:

— security audit (AUD);

— protection of information (automated) system and its components (ZIS);

— information security incident response (INTs);

— staff informing and training (IPO).

It should be mentioned that the decision on the ISPS completeness to a certain extent depends on the financial capacities of the enterprise. However, if the cost of the protected resources and the potential damage from hazards is higher than the cost of the ISPS, then it makes sense to implement AUD and ZIS.

Comparative analysis of the FSTEC Order no. 239 of December 25, 2017, and 800-82 Revision 2 Guide to Industrial Control Systems (ICS) Security is given in Table 2.

Table 2

Elements (subsystems) of enterprise IS protection system in
FSTEC Order no. 239 of December 25, 2017, and in 800-82 Revision 2
Guide to Industrial Control Systems (ICS) Security)

	FSTEC Order no. 239 of 25.12.17	800-82 Revision 2 Guide to ICS Security
ISPS Subsystems	Identification and authentication (IAF) Identification and authentication	
	Access control (UPD) System and communications protection, Security assessment and authorization	
	Restriction of software environment (OPS)	System and information integrity
	Protection of machine-readable media (ZNI) Media protection	
	Security audit (AUD) Auditing and accountability	
	Antivirus protection (AVZ)	System and information integrity
	Intrusion prevention (hacking) (SOV)	System and information integrity
	Protection of information (automated) system and its components (ZIS)	System and information integrity
	Integrity control (OTsL)	System and information integrity
	Information assurance (ODT) System and services acquisition	
	Event planning to ensure information protection (PLN) Planning, contingency planning	
	Protection of technical facilities and systems (ZTS) Maintenance	
	Information security incident response (INTs) Incident response	
	Personnel informing and training (IPO) Personnel security	
	Software update control (OPO)	Organization — wide information security program management controls
	Security protection of emergency procedures (DNS) Physical and environmental protection Awareness and training	
	Configuration control (UKF) Configuration management	
	—	Risk assessment
	—	System and communications protection

Note. For greater clarity, variances are not only placed in different cells, but are also highlighted in gray.

In this case, the following differences are most obvious:

— 800-82 Revision 2 Guide to ICS Security combines the functional of the subsystems of OPS, AVZ, SOV, OTsL, ZIS defined in the FSTEC Order, in the subsystem of "System and information integrity";

— 800-82 Revision 2 Guide to ICS Security provides a subsystem for the protection of communication systems — "System and communications protection";

— The FSTEC Order combines the functional of the subsystems "System and communications protection" and "Security assessment and authorization" in the "Access control subsystem (UPD)";

— The FSTEC Order combines the functional of the "Planning" and "Contingency planning" subsystems in the subsystem of "Event planning to ensure information protection (PLN)";

— The FSTEC Order combines the functional of the subsystems of "Physical and environmental protection" and "Awareness and training" in the subsystem of "Security protection of emergency procedures (DNS)".

Special mention should be made of the subsystems for risk assessment and protection of communication systems [10]. These are the critical items of the enterprise IS protection system among those that are not provided for by domestic regulatory documents. Their implementation will enable to enhance protection; to respond promptly to incidents that arise in the enterprise IS; to counteract attacks timely and accurately.

Discussion and Conclusions. The analysis results of the IS protection system components will be used to build a model of intellectual support for decision-making when designing the ISPS. Particularly, it is planned to foresee the possi-

bility of expanding the ISPS subsystem setup. The selection of the system units will depend on the risk assessment, the extent of potential damage by injurious actions, and the cost of the ISPS components.

References

1. Ovsyanitskaya, L.Yu., Podpovetnaya, Yu.V., Podpovetnyy, A.D. Information security of small business: modern condition, problems and the ways of their colutions. Bulletin of the South Ural State University (Series “Computer Technologies, Automatic Control & Radioelectronics”), 2017, no. 4, pp. 77–84.

2. Glukhov, V.V., Ilin, I.V., Anisiforov, A.B. Problems of data protection in industrial corporations enterprise architecture. SIN'15: Proceedings of the 8th International Conference on Security of Information and Networks. New York ACM, 2015, pp. 34–37.

3. Pishchik, B.N. Bezopasnost' ASU TP. [Security of automated control systems for technological processes.] Computational Technologies, 2013, vol. 18, spec.iss., pp. 170–175. Available at: file:///C:/Users/User/Downloads/23%20Pishik_n.pdf (accessed: 22.07.18) (in Russian).

4. Gritsay, G., et al. Bezopasnost' promyshlennykh sistem v tsifrakh. [Safety of industrial systems in figures.] Moscow: Positive Technologies, 2012, 37 c. Available at: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (accessed: 22.07.18) (in Russian).

5. Mukminov, V.A., Khutsishvili, V.M., Lobuzko, A.V. Metodika otsenki real'nogo urovnya zashchishchennosti avtomatizirovannykh system. [Methods of the assessment of mis real protection levels.] Software & Systems, 2012, no. 1 (97), pp. 39–42 (in Russian).

6. Lukatskiy, A. Obzor mirovykh standartov IB ASU TP i sovety po ikh primenimosti v rossiyskikh usloviyakh. [Survey of IS world standards of automatic process control systems and hints on their applicability in Russia’s circumstances.] Cisco Systems: Docplayer. Available at: http://docplayer.ru/33122677-Obzor-mirovyh-standartov-ib-asu-tp-i-sovety-po-ih-primenimosti-v-rossiyskih-usloviyah.html (accessed: 22.07.18) (in Russian).

7. Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v av-tomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy : Prikaz Federal'noy sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. № 31. [On Approving Requirements for Providing Information Protection in Automated Control Systems of Production and Technological Processes at Critical Objects, Potentially Hazardous Facilities, and Objects posing high threat to life and health of people and the environment: Order no. 31 of the Federal Service for Technology and Export Control of March 14, 2014.] Federal Service for Technology and Export Control. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed: 22.07.18) (in Russian).

8. Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz Federal'noy sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 25 dekabrya 2017 g. № 239. [On Approval of Requirements for Ensuring the Security of Significant Facilities of the Information Infrastructure of the Russian Federation: Order no. 239 of Federal Service for Technology and Export Control of December 25, 2017.] Federal Service for Technology and Export Control. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/1593-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed: 22.07.18) (in Russian).

9. Stouffer, K., et al. Guide to Industrial Control Systems (ICS) Security. U. S. Department of Commerce; National Institute of Standards and Technology. Gaithersburg: NIST, 2015, 247 p.

10. Singhal, A., Ou, X. Security risk analysis of enterprise networks using probabilistic attack graphs. Network Security Metrics. Cham: Springer, 2017, pp. 53–73.

Received 21.06 .2018
Submitted 25.06.2018
Scheduled in the issue 20.07.2018

Authors:

Vitenburg, Ekaterina A.,
postgraduate student of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF),
ORCID: https://orcid.org/0000-0002-1534-8865
e.vitenburg@ec-rs.ru

Levtsova, Alexandra A.,
student of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF),
ORCID: https://orcid.org/0000-0002-4798-9704
alexandra.levtsova@yandex.ru